Response to the amdflaws publication

By Ilia Luk-Zilberman – CTO @ CTS-Labs

Disclaimer – I am a technical guy, I love building things, and researching things. I do not like the whole world of PR, it is too messy for me. I have written this letter in my own language, without PR proofing, please forgive me if there are any grammatical errors, or not written according to correct writing standards.

History of the publication – we have started researching ASMedia chips about a year ago. After researching for some time, we have found manufacturer backdoors inside the chip which give you full control over the chips (ASM1042, ASM1142, ASM1143). We wanted to go public with the findings, but then saw that AMD have outsourced their chipset to ASMedia. So we decided to check the state of AMD, we bought a Ryzen computer, and whimsically ran our exploit PoC, and it just worked out of the box. Full Read/Write/Execute on the AMD Chipset, as is – no modifications. To be honest, we were a bit shocked by it, how they have not removed the backdoors when integrating ASMedia IP into their chipset is beyond me. So then we said, ok – what on earth is going on in AMD, and started researching AMD.

It took time to set-up the working environment to start communication with the AMD Secure processor, but after reaching a full working setup and understanding of the architecture – we started finding vulnerabilities. One, and another and another. And not complex, crazy logical bugs, but basic mistakes – like screwing up the digital signatures mechanism. At that point, about once a week we found a new vulnerability, not in one specific section, but across different sections and regions of the chips. It's just filled with so many vulnerabilities that you just have to point, research, and you'll find something (obviously a personal opinion).

After that we decided we have to go public with this. I honestly think it's hard to believe we're the only group in the world who has these vulnerabilities, considering who are the actors in the world today, and us being a small group of 6 researchers.

Responsible Disclosure

I know this is an extremely heated topic for debate, where everyone has a strong opinion. Unfortunately, I also have a strong opinion on this topic.

I think that the current structure of "Responsible Disclosure" has a very serious problem. If a researcher finds a vulnerability, this model suggests that the researcher and the vendor work together to build mitigations, with some time limit (30/45/90 days), at the end of which the researcher will go out with the vulnerabilities. The time limit is meant to hasten the vendor to fix the issues.

The main problem in my eyes with this model is that during these 30/45/90 days, it's up to the vendor if it wants to alert the customers that there is a problem. And as far as I've seen, it is extremely rare that the vendor will come out ahead of time notifying the customers – "We have problems that put you at risk,

we're working on it". Almost always it's post-factum – "We had problems, here's the patch – no need to worry".

The second problem is - if the vendor doesn't fix it in time – what then? The researcher goes public? With the technical details and exploits? Putting customers at risk? How we have accepted this mode of operation is beyond me, that researchers advertise at the end of the time limit the technical details of the vulnerabilities "because" the vendor didn't respond. Why should the customers pay for the vendor's lack of actions. I understand – this is the model today and people follow suit, but I think we can do better.

I think that a better way, would be to notify the public on day 0 that there are vulnerabilities and what is the impact. To notify the public and the vendor together. And not to disclose the actual technical details ever unless it's already fixed. To put the full public pressure on the vendor from the get go, but to never put customers at risk.

This model has a huge problem; how can you convince the public you are telling the truth without the technical details. And we have been paying that price of disbelief in the past 24h. The solution we came up with is a third party validation, like the one we did with Dan from trailofbits. In retrospect, we would have done this with 5 third party validators to remove any doubts. A lesson for next time.

I know there are many questions, and a whole lot of confusion. We are trying our best to answer reporters, update our site with Q&A, and clarify what's going on. So far the media focus was on CTS, and I think I understand this, but very soon we will have to deal with the fact that a huge company with products spread throughout millions of computers in the world, is riddled with so many problems that it's unclear how to even address this.

If you have any technical questions, please contact me at ilialuk@cts-labs.com, I'll try to answer as many questions as I can.